REMARKS

Claims 1-6, 8-18 and 20-25 remain pending in the present application. Claims 1, 11, 15, 20 and 25 are independent claims. Applicant requests reconsideration and allowance in view of the foregoing amendments and the following remarks.

Rejection under 35 U.S.C. § 103(a) based on Fischer, Goodman, Menzes and Nakamura

On pages 2-7, the Action rejects claims 1-6, 8-18 and 20-25 under 35 U.S.C. 103(a) as allegedly being unpatentable over Fischer (U.S. Patent No. 5,001,752) in view of Goodman (U.S. Patent No. 5,001,752), Menzes (Handbook of Applied Cryptography), and Nakamura (U.S. Patent No. 6,457,126). Applicant respectfully traverses this rejection.

For at least the following reasons, Applicant disagrees with the assertions made in the Office Action alleging that the cited references in combination render claim 1 obvious under 35 U.S.C. § 103(a).

As previously stated, the combined teachings of Fischer and Goodman do not teach providing an encryption processor that uses a single secure encryption key to perform different operations in multiple modes, in contrast with the statements made by the Final and Advisory Actions. Specifically, Goodman does not teach or suggest "the processor operable in a first mode wherein the **secure encryption key** is used for encryption operations and for test operations and in a second mode in which the **secure encryption key** is only used for timestamping operations," as recited in claim 1. The following discusses the teachings of Fischer and Goodman as they relate to claim 1.

In FIG. 1, Fischer discloses a processor module 6 coupled to a storage device 8. The storage device stores a secret private key of a public/private key pair (also see Fischer, col. 4, lines 35-38). However, Fischer does not teach using the secret private key in multiple modes. Fischer also does not teach the processor module 6 using the secret private key in a first mode for

encryption operations and for test operations and in a second mode in which the secret private key is only used for timestamping operations.

The Actions rely on Goodman for a teaching of these features. In its analysis, the Advisory Action states that Goodman is "merely relied upon for its teaching of multiple modes," however, Fischer lacks more than a teaching of multiple modes. Fischer also lacks a teaching of the processor module 6 respectively performing the claimed encryption, test, and timestamping operations in the multiple modes using a **single key**.

However, Goodman does not provide such a teaching of an encryption processor performing the claimed operations in different modes using a **single key**. Instead, Goodman teaches an encryption processor useable in two modes, the test mode using a **private test key**, and the work mode using a separate **secure electronic key** (see Goodman, col. 5, lines 14-20, col. 5, lines 62-col. 6, line 2, col. 6, lines 55-56, also see col. 7, lines 15-28). Goodman also teaches a pseudo test mode that is not a true test mode (see Goodman, col. 8, lines 53-67). Goodman further teaches that once the test mode has been entered, test data, including the **private test key**, is provided to the integrated circuit 20 via test port 27 and is stored in the volatile memory circuit 24. Goodman teaches that **during the test mode**, the **secure electronic keys** are **inaccessible** (see Goodman, col. 7, lines 53-55, col. 8, lines 48-52).

However, Goodman teaches using the **private test key** in the test mode, but does not teach or suggest using the private test key in the *work* mode. Likewise, Goodman teaches using the **secure electronic key** in the work mode, but does not teach or suggest using the secure electronic key in the *test* mode. Thus, Goodman teaches using **separate keys** in **separate respective modes**. Nowhere does Goodman teach using a **single key** in **multiple modes**. Specifically, Goodman does not teach that the encryption processor 23 (or 33, 43, 66) using a private test key (or a secure electronic key) in a first mode for encryption operations and for test operations and in a second mode in which the private test key (or the secure electronic key) is only used for timestamping operations. Therefore, Fischer in light of Goodman does not teach all of the claim features.

On page 4 of the present Office Action, the Office concedes that the modified Fischer, Goodman, and Meezes system fails to disclose the same key is used in bothe modes. The Office states that Nakamura teaches a key used in two modes in col. 15, lines 66 through col. 16. line 5, and col. 17, lines 9-26, and asserts that at the time of the invention it would have been obvious to one skilled in the art to use the same key in both modes of the modified Fischer, Goodman, and Menzes system. As Nakamura explains from col. 15, line3 66 to col. 16, line 5, "the controlling section 162 performs addition (K1 + k2) of the data key K1 to the system k2, connection (K1 ; k2), and multiplication (K1 * k2), etc. in order to generate a new encryption key, and encrypts data using the generated key. Otherwise, the controlling section 162 encrypts data using the data key K1, and encrypts the encrypted data using the system key k2." Applicants respectfully submit that this, or any other Nakamura disclosure fails to teach or reasonably suggest the use of a **single key** in multiple modes for **test, encryption, and timestamping**, as set forth in claim 1.

Again, as previously explained, the only teaching of providing a processor that uses a **single key** in multiple modes for test, encryption, and timestamping operations is found in Applicant's disclosure. Based on the teachings of Fischer and Goodman, assuming, *arguendo*, that there is motivation to combine these references, one of ordinary skill in the art would not modify the references as alleged by the Action. One of ordinary skill in the art might modify the processor module 6 of Fischer to have two modes and use the secret private key of Fischer in the work mode, similar to that of Goodman, and add a test mode to the processor module 6 of Fischer to use the private test key in the test mode, similar to that of Goodman. Thus, assuming that proper motivation to combine could be found, the combined teachings might suggest using separate keys in separate modes. However, this modification does not teach or suggest providing a processor that uses a **single key** in different operations in different modes. The Action impermissibly relies on Applicant's own disclosure to bridge this gap between the teachings of Fischer in view of Goodman and the claimed invention. Without Applicant's teachings of providing a processor that uses a **single key** in multiple modes for different operations, one of

ordinary skill in the art would not modify the combined teachings of Fischer and Goodman as stated in the Action to render claim 1 obvious. Additionally, Menezes does not teach an encryption processor using a single key in multiple modes to supplement Fischer and Goodman. Nakamura also does not tach an encryption processor using a single key in multiple modes to supplement Fischer and Goodman. Thus, the combined teachings of Fischer, Goodman, Menezes, and Nakamura do not teach or suggest the features of claim 1, in contrast with the statements of the Action.

Applicant respectfully submits that the Office has improperly applied individual parts of Goodman, Fischer, Menezes and Nakamura as a mosaic to recreate a facsimile of the invention. It is well known that it is improper to use the claims as a frame, and use individual parts of prior art as a mosaic to recreate a facsimile of the invention. *Interconnect Planning Corp. v. Feil*, 227 USPQ 2d 543, 551 (Fed. Cir. 1985).

Applicant notes that a further description of Fischer, Goodman, and Menezes was included with the previous Amendment filed June 24, 2005, the Request for Reconsideration filed October 28, 2005, and the Pre-Appeal Brief Request for Review filed November 28, 2005. Applicant respectfully requests that the Examiner also reconsider the arguments presented in the previous filings, which are not included herein, for brevity. Thus, for at least the reasons stated above, the combined teachings of Fischer, Goodman, Menezes, and Nakamura do not teach or suggest all of the features recited in claim 1. Therefore, the Action does not establish a *prima facie* case of obviousness to reject claim 1 under 35 U.S.C. § 103(a) based on the combined teachings of Goodman, Fischer, Menezes and Nakamura.

Accordingly, claim 1 is allowable over the cited references and allowance thereof is respectfully requested. Claims 2-6 and 8-10, which depend from claim 1, are also in condition for allowance because of their dependence on an allowable claim.

Claim 11 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested. Claims 12-14, which depend from claim 11, are also in condition for allowance because of their dependence on an allowable claim.

Claim 15 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested. Claims 16-18, which depend from claim 15, are also in condition for allowance because of their dependence on an allowable claim.

Claim 20 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested. Claims 21-24, which depend from claim 20, are also in condition for allowance because of their dependence on an allowable claim.

Claim 25 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested.

Applicant requests reconsideration and withdrawal of the rejection of claims 1-6, 8-18 and 20-25 under 35 U.S.C. § 103(a) as being unpatentable over Goodman, Fischer, Menezes and Nakamura.

Conclusion

All of the stated grounds of rejection have been properly traversed. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is hereby invited to telephone the undersigned at the number provided.

The Patent Office is hereby authorized to charge the fee for a ONE-month extension of time to Deposit Account No. 22-0261. No additional fees are believed to be required. However, if the Office deems that any fees are necessary, authorization is hereby granted to charge any required fees to Deposit Account No. 22-0261.

Prompt and favorable consideration of this Amendment is respectfully requested.

April 24, 2006

Respectfully submitted,

By _____
James R. Burdett
Registration No. 31,594
Thomas C. Schoeffler
Registration No. 43,385
VENABLE LLP
P.O. Box 34385
Washington, DC 20043-9998
Attorney/Agent for Applicant

JRB/TCS